REMARKS

I. Introduction

In response to the Office Action dated June 11, 2008, claims 1, 17, 30 and 46 have been amended. Claims 1-58 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Objections

In paragraph (3) of the Office Action, claims 30 and 46 were objected to because of certain informalities in the preamble.

Applicant's attorney has amended claims 30 and 46 to overcome these objections.

III. Prior Art Rejections

In paragraph (3) of the Office Action, claims 1, 17, 21, 25, 30, 46, 50, and 54 are rejected under 35 U.S.C. §103(a) as being unpatentable over Voltmer et al., U.S. Publication No. 2002/0112177 (Voltmer) in view of Flink et al., U.S. Patent No. 7,024,562 (Flink), in view of Hamid, U.S. Publication No. 2003/0091218 (Hamid), and in view of Epstein, U.S. Publication No. 2002/0124176 (Epstein). In paragraph (4) of the Office Action, claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, and 55-58 are rejected under 35 U.S.C. §103(a) as being unpatentable over Voltmer, in view of Flink, in view of Hamid, in view of Epstein, and in view of Musgrave et al., U.S. Patent No. 6,202,151 (Musgrave).

Applicant's attorney respectfully traverses these rejections.

Applicant's claimed invention is patentable over the combination of references, because the claims contain limitations not taught by the combination. Specifically, Applicant's invention is designed to enable the authorized submission and authentication of biometric data in a confidential manner. In this regard, the biometric data is processed by an irreversible cryptographic algorithm causing the resulting data to be undecipherable, irreversible and undecryptable, but still capable of being used for comparison purposes. Moreover, all traces of the unprocessed biometric data are eliminated from the system and storage prior to any comparison.

The Office Action, on the other hand, asserts that the combination of Voltmer, Flink, Hamid and Epstein describes all the limitations of Applicant's independent claims:

> 3. Claims 1, 17, 21, 25, 30, 46, 50 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voltmer et al. (US Pub. No. 2002/0112177) in view of Flink et al (US Patent No. 7,024,562) in view of Hamid (US Pub. No. 2003/0091218) and in view Epstein (US Pub. No. 2002/0124176).
>
> As per claim 1, Voltmer teaches: an anonymous biometric authentication system and method for receiving a first biometric data and a second biometric data [Fig. 1-3, 12A, 12B, paragraph 0010, 0013]; comparing the second data to the first data and generating a signal pertaining to the comparison of the second data to the first data for use in an authentication process [paragraph 0013, 0017, 0051]. Voltmer teaches converting and/or encrypting the biometric data [paragraph 0046 lines 13-17]; discarding the credentials after the enrollment stage [paragraph 0045, 0053]. Voltmer doesn't expressively mention that processing the first biometric data combined with the first personal key. Flink teaches: processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data; processing the second biometric data combined with the second personal key through an irreversible cryptographic algorithm to form a second processed data and comparing the second processed data to the first processed data [Fig. 3, col. 8 lines 13-31]. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Voltmer's invention according to Flink's teachings. One skilled would have been motivated to incorporate Flink's teachings because it improves the security and provides higher security level [Flink, col. 4 lines 13-22]. Voltmer and Flink don't expressively mention comparing the second processed data to the first processed data, without accessing the first and second processed data in an unprocessed form. Hamid teaches: comparing the second processed data to the first processed data, without accessing the first and second processed data in an unprocessed form, in order to enable authentication of the first and second biometric data in a confidential manner [Fig. 9, 10, 11, paragraph 0078, 0079].
>
> It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Voltmer's and Flink's invention with the teachings of Hamid, to prevent security attacks because Hamind's method that does not necessitate the storage of templates against which a fingerprint is compared [Hamid, paragraph 0020]. Hamid teaches storing the hashed enrollment value only. Hamid doesn't expressively mention eliminating all storage or trace of the unprocessed data. Epstein teaches eliminating all storage or trace of the unprocessed data [Fig. 4, paragraph 0029]. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Voltmer's, Flink's and Hamid's invention with the teachings of Epstein to provide a biometric authentication and access security method that is less susceptible to forged or copied biometric information [Epstein, paragraph 0008].

Applicant's attorney disagrees with this analysis.

Voltmer describes the comparison of biometric data, as well as the encryption of biometric data for storage and transmission. However, nowhere does Voltmer describe the comparison of encrypted biometric data, without accessing the biometric data in unencrypted form. The Office

Action's assertion that Voltmer performs this function is unsupported by any explicit discussion in Voltmer, and merely comprises a hindsight inference by the Office Action.

As admitted in the Office Action, Voltmer does not mention encrypting (processing) the combination of biometric data and a personal key. However, the Office Action errs when it asserts that Flink teaches these limitations.

Instead, Flink merely describes adding a biometric sample to digital documents, and then passing the digital documents and the biometric sample through a hash function to produce a seal. However, the digital documents used in Flink are nowhere described as being personal keys, as recited in Applicant's claims.

Moreover, as admitted in the Office Action, Voltmer and Flink do not mention comparing the second processed data (the encrypted combination of the second biometric data and the second personal key) to the first processed data (the encrypted combination of the first biometric data and the first personal key), without accessing the first and second processed data in an unprocessed (unencrypted) form. However, the Office Action errs when it asserts that Hamid teaches these limitations.

Instead, Hamid merely describes the hashing of a biometric information sample, but does not hash a personal key in combination with the biometric information sample. The unhashed biometric information sample in Hamid is used for comparison purposes in FIG. 10 of Hamid, where the enrolled string, not the hashed string, is used in the verification, while FIG. 11 of Hamid shows the generation of multiple strings from biometric data, where the multiple strings are hashed and then compared to the stored hash string. Moreover, these strings are accessed in both unhashed and hashed forms, which differs from Applicant's claims' requirement that all storage or trace of the biometric data in an unprocessed form be eliminated, and that the comparisons be performed only on encrypted data without accessing the unencrypted data.

In addition, the Office Action errs when it asserts that it would be obvious to modify Voltmer and Flink with the teachings of Hamid, to prevent security attacks because Hamid stores the hashed enrollment value only (even though the Office Action admits that Hamid does not eliminate all storage or trace of the unprocessed data), because Epstein teaches eliminating all storage or trace of the unprocessed data.

Instead, Epstein merely describes a token device that is used in conjunction with an individual's biometric information for authentication and access security. However, Epstein only describes the comparison of encrypted random numbers, not the comparison of an encrypted combination of biometric data and personal keys. Moreover, Epstein refers to the discarding of the biometric information and the private key after the private key has been decrypted using the biometric information and after the random number has been encrypted using the private key. Nonetheless, during those decrypting and encrypting steps, both the biometric information and the private key are used in unencrypted form in Epstein, unlike Applicant's claimed invention.

Thus, when combined, Voltmer, Flink, Hamid and Epstein describe something different from Applicant's claimed invention, namely the comparison of biometric data without a personal key and without eliminating all storage or trace of the biometric data in an unprocessed form (Voltmer); the encryption of biometric data without a personal key for storage and transmission (Voltmer); the addition of biometric data to digital documents to produce a seal (Flink); the hashing of a biometric information sample without a personal key and without eliminating all storage or trace of the biometric data in an unencrypted form (Hamid); and the comparison of random numbers encrypted by a private key that itself is encrypted by biometric data, the use of the private key and biometric data in unencrypted form for encryption and decryption, and the discarding of the unencrypted private key and biometric data only after the encryption and decryption has been performed (Epstein).

Applicant's invention, on the other hand, does not allow recovery of the biometric data and personal key in its unprocessed (decrypted) form. Instead, Applicant's invention is directed to protecting the biometric data and personal key from being captured and revealed (a) while in transit; (b) while stored in a database; and (c) during the comparison. In this regard, Applicant's invention eliminates all storage and traces of the biometric data and personal key after they are irreversibly encrypted and before the comparison is performed.

Further, Applicant's attorney submits that Voltmer, Flink, Hamid and Epstein cannot be combined in the manner asserted by the Office Action. Any attempt to combine the Voltmer, Flink, Hamid and Epstein references would render them operable and incapable of performing the tasks for which they were devised. Consequently, the Voltmer, Flink, Hamid and Epstein references cannot be combined to teach Applicant's claimed invention.

Musgrave fails to overcome the deficiencies of Voltmer, Flink, Hamid and Epstein. Recall that Musgrave was cited only against dependent claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, and 55-58, and only for teaching the various limitations of these dependent claims, but not the independent claims.

Thus, Applicant's attorney submits that independent claims 1, 17, 30 and 46 are patentable over Voltmer, Flink, Hamid, Epstein and Musgrave. Further, dependent claims 2-16, 18-29, 31-45 and 47-58 are submitted to be patentable over Voltmer, Flink, Hamid, Epstein and Musgrave in the same manner, because they are dependent on independent claims 1, 17, 30 and 46, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-16, 18-29, 31-45 and 47-58 recite additional novel elements not shown by Voltmer, Flink, Hamid, Epstein and Musgrave.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicant's undersigned attorney.

It is believed that no fees are due at this time. Nonetheless, should any charges be deemed necessary, please charge any such fees, or credit any overpayments, to Deposit Account No. 09-0460 of IBM Corporation.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: September 11, 2008

By: /George H. Gates/
Name: George H. Gates
Reg. No.: 33,500

GHG/

G&C 30571.302-US-U1